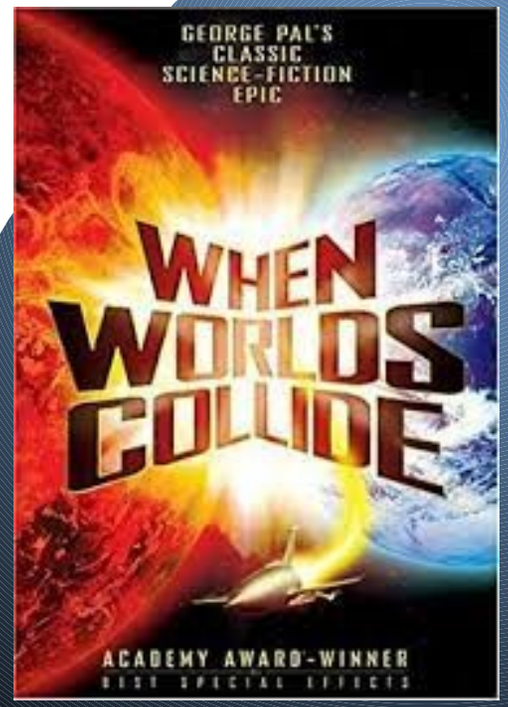
Zero Trust and PAM: When Worlds Collide

Dr. Fred Cohen
CEO Management Analytics
2022-05-17
fc@manalyt.com
+1-831-200-4006

Privileged Access Management

chmod 755 usr/bin/pkexec



Zero Trust

Management Analytics

ALL.NET

What is Zero Trust

Trust

The willingness to be harmed by someone/thing

Dictionary: firm belief in the reliability, truth, ability, or strength of someone or something.

Zero Trust

No willingness to be harmed by anyone/thing

No belief in the reliability, truth, ability, Or strength of anyone / anything

So-called Zero Trust

A misnomer / deceptive in nature

Aggregating risk in a smaller number of things that are then de-facto trusted

Thinking about trust

Don't trust "zero trust"

In reality, we trust certain things/people for certain purposes for periods of time

Conclusion: "Zero trust" is goblety goop – Don't trust it

"I have zero trust in their approach.
In large part, because they have 'zero trust' in their approach."

Management Analytics

ALL.NET

We cannot live without trust!

- http://all.net/ “Theorem 0 – I Exists (trust me)”
  - We use computers → there is a non-zero consequence
    - Thus we trust them (to some extent for some purpose)
  - They are based on physics (a theory we trust)
    - They operate in hardware (a mechanism we trust)
      - They run software (mechanisms we trust)
        - We use them (we trust ourselves)
          - They communicate (a media we trust)
            - All these were built by other people (we trust)
              - They trusted other people
- We must trust – but what do we trust for what?
  - How do we model it?
    - How do we rely on it?
      - What are its limits?

Why would I ever have to do this:
chmod 755 usr/bin/pkexec

What is Privileged Access Management

PAM

We trust people/things by giving them access

All access is associated with “privileges”
We have to manage that access appropriately

What is “appropriately”?

Higher consequences → More trust (and access)

We should grant privileges only when needed
And only when the risks balance the trust

Note: Who do we trust to decide?

What is “Risk”?

The variance in (envelope of) possible futures

We take risks for rewards
We “trust” to gain the rewards

How do we balance trust and risk?

We can be ad-hoc or systematic

Hint: Systematic – why?

To be systematic we need to create a system
The system of trust and basis → “PAM”

Note: Complexity v. Granularity

Conclusion: “PAM” is about systematic trust with basis

What kind of basis?

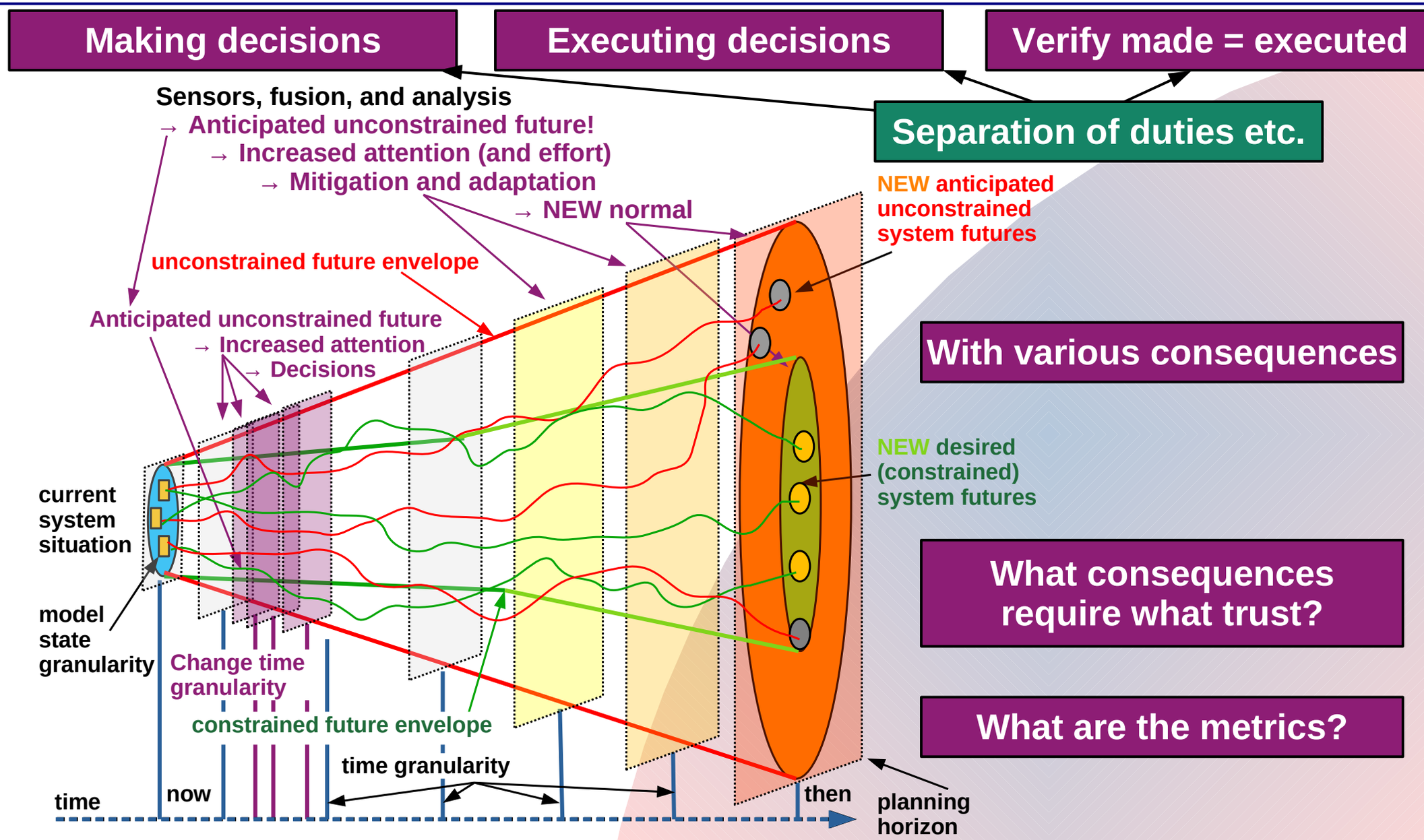
The standards of practice approach
http://all.net/SoP/SecDec/ControlArch4.html

Party	Risk level (purposes)	Trusted based on
Business	Low	Historic behavior (e.g., credit rating and internal experiences) and group memberships (i.e., chamber of commerce, business groups, exchange memberships) or convenience
Business	Medium	Contracts, historical behavior, size (deep pockets), legal suitability
Business	High	Contracts, transparency, historical behavior, size (deep pockets), legal suitability, systematic background checks, and executive risk acceptance
People	Low	Contracts and group membership, expertise, or transitive trust chains
People	Medium	Historical behavior,expertise, systematic background checks, and contracts
People	High	Historical behavior, expertise, systematic background checks, psychological factors, external clearances, contracts, and sometimes nationality
Systems	Low	Historical behavior, contracts, transitive trust chains (someone told me it was good, a magazine review, etc.)
Systems	Medium	Historical behavior, transparency transitive trust chains (authors, reputations, reviews, etc.), chain of custody, contracts
Systems	High	Historical behavior, transparency, transitive trust chains (authors), chain of custody, contracts, and certifications (CC, TCSEC, TCG, etc.)
Content	Low	Transitive trust chains, transparency, metadata
Content	Medium	Historic behavior (of the source), transparency, chain of custody, group memberships (of the author), credentials (of the author), contracts, metadata, form and format
Content	High	Investigation (scientific demonstrations), historic behavior (of the source), transparency, chain of custody, group memberships (of the author), credentials (of the author), contracts, metadata, form and format, diplomatic analysis

Trust model - What is the basis for trust?

Hint: The "basis" must include adjudication rules and adjudicators
And we have to trust them to some extent… and on and on

Trusted for what?



What about limited trust?

- Making decisions:
  - What about risk aggregation?
  - What about separation of duties?
  - What about change management?
  - What about … lots of other things
- Executing decisions
  - Inventory
  - Work flows
  - Time vs. surety
  - Cost vs. surety
  - Matching surety to consequences

Trust but verify?
But who shall check the checkers?

Unreasonable
Reasonable

Prudent
Imprudent

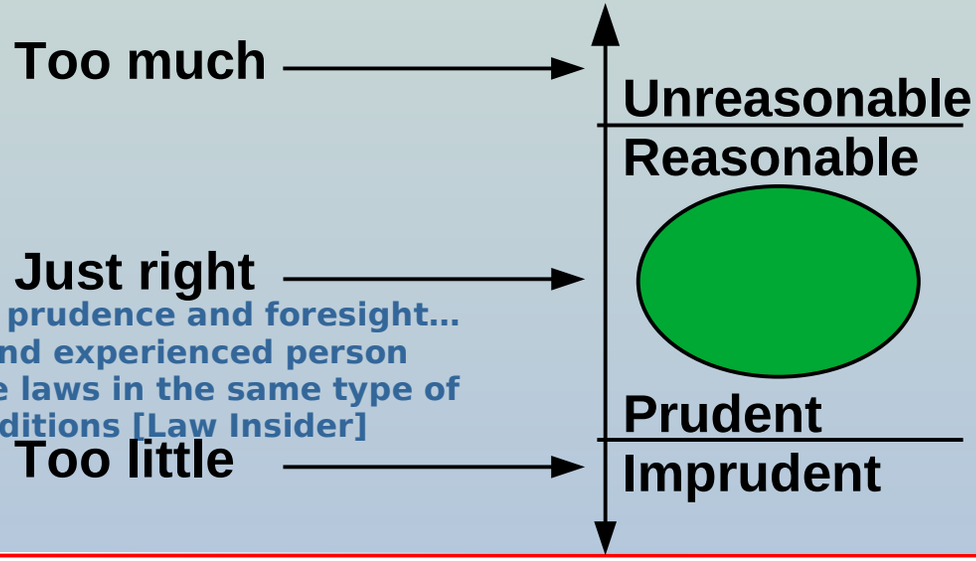
Decisions are made by executives
Or delegated de-facto or otherwise

We place trust in all of these mechanisms – a net improvement?

Due diligence (not negligent)

- Due diligence
  - → Reasonable and prudent
    - **Reasonable** steps taken by a person in order to satisfy a legal requirement, especially in buying or selling something. [Oxford languages]
    - The care that a **prudent** person might be expected to exercise in the examination and evaluation of risks affecting a business transaction [Findlaw]
- Reasonable and prudent
  - Situation-dependent
  - The right amount
  - **In relation to an undertaking,… [use of] skill, diligence, prudence and foresight… reasonably and ordinarily … exercised by a skilled and experienced person complying with recognized standards and applicable laws in the same type of undertaking under the same circumstances and conditions [Law Insider]**

Situation dependent
Seriously considered
By an expert
In light of history



Organizational Decision-making Design

Ownership and Board Cognitive System

Intent: Self image and World image / Knowledge, theories, models of people, systems, and the World

Objectives: (Assessment → Defined problems) Board sets values and vision. Vision, Objective performance and growth goals and identifies overall strategic objectives.

Schedule: (Urgency → Timing) Board identifies strategic time frames for identified objectives.

Budget: (Importance → Spending) Board reviews and opines on budgets and uses internal audit to verify that expenditures are

Information is received by the Chairman and

Decision Time Frames
Emergency: Hours
Urgent: Days
Timely: Weeks
Day-to-day: Quarters
Periodic: Quarters
Occasional: Years

→ Decisions are made and executed by the Voting Members

They provide outbound Influence and Sharing →

They provide internal Advice and Influence and Requirements and Directives ↓

Ownership Control

Understand Business and Define Duties

Executive Decisions

It's unavoidable

Someone is in charge (legally)
We "trust" them by legal mandate

They need to make decisions
They can delegate, etc. but...

The buck stops there
Even if it is a committee

We "trust" the executives
By them making the decisions

But even if it were a majority vote
We still "trust" the voters

We are forced to trust the deciders
Otherwise we cannot function

How do we manage the trust?

The organization must function

Management control → Trust

Access management → Human

Owners/Board/Execs decide

NOTE: Matching I/O and [timing→consequences]

Top Management Cognitive System

Decision Time Frames
Emergency: Minutes
Urgent: Hours
Timely: Days
Day-to-day: Weeks
Periodic: Quarters
Occasional: Quarters

↓ They receive internal Advice and Influence and Requirements and Directives

→ Decisions are made and executed by the CEO and Executive Team

They provide outbound Influence and Sharing →

provide internal Advice and Influence and

ements and Directives and Policy ↓

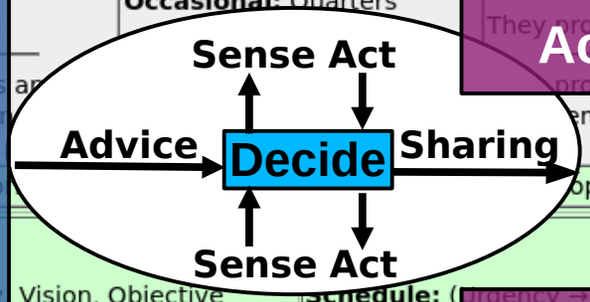
Executive Control

Understand Business and Define Duties and Manage

Risk and Specify

Verify

Operations



Intent: Self image and Wo ople, systems, and the World

Objectives: (Assessment → Defined problems) and assess performance and growth goals and form overall strategic objectives. Top management roll-ups and as a committee forms internal paths forward and assignments for completing those tasks.

Quality: (Personality Vision, Objective Driven) Based on board-specified quality d codifies and promulgates vision and mission.

Schedule: (Urgency → Timing) Based on long-term strategy, CE for the top executive team and sets time requirements on completion.

Budget: (Importance → Spending) CEO works with top executive team to identify tent with the tactics and planning of other top executives.

Management Analytics

ALL.NET

PAM automates the execution (sort of)

PAM

It's unavoidable

100M+ protection bits on each system
Often thousand or more systems

We cannot "manually" grant access
We cannot "manually" remove access

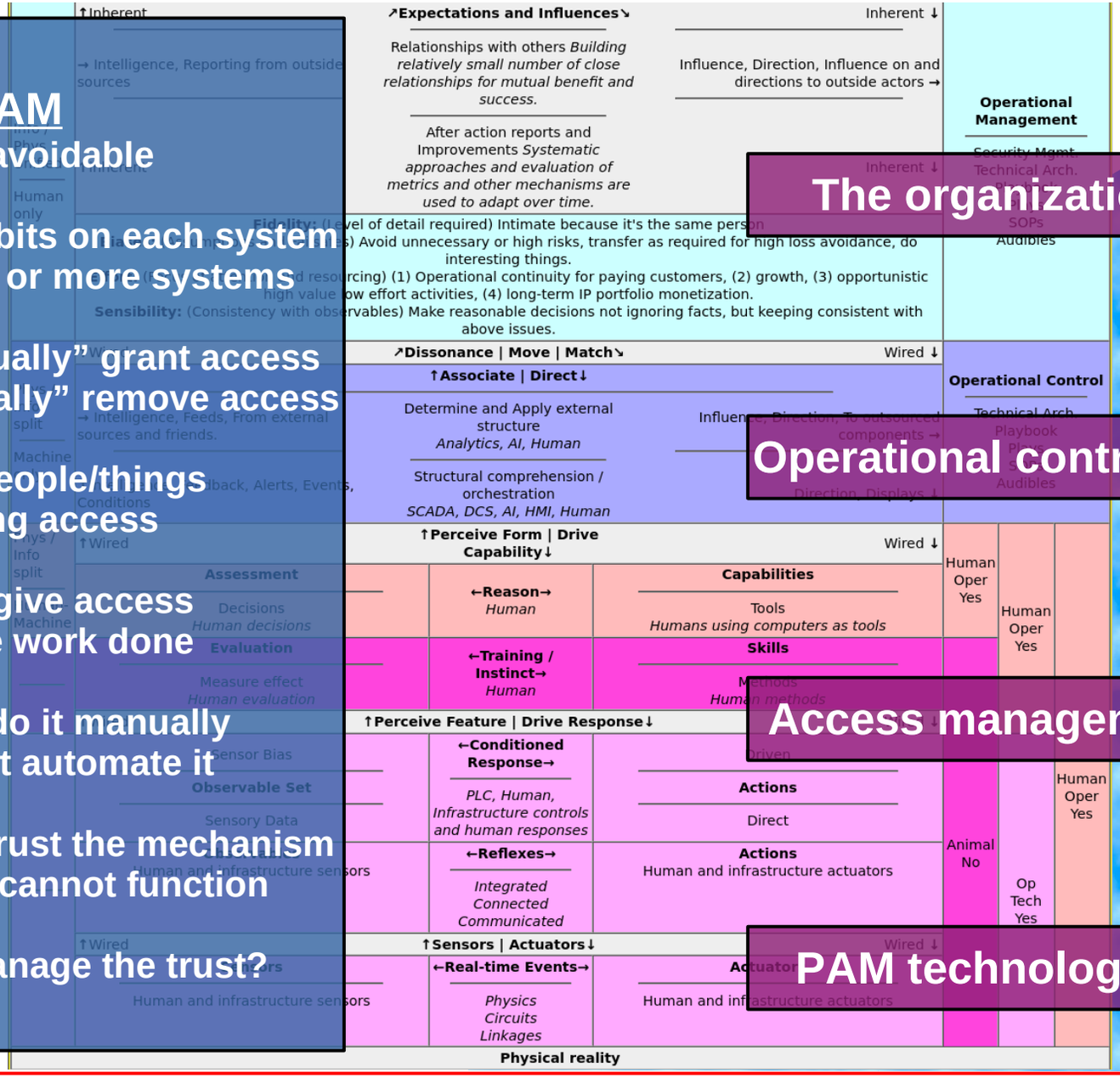
We trust people/things
By giving access

We must give access
To get the work done

We cannot do it manually
So we must automate it

We are forced to trust the mechanism
Otherwise we cannot function

How do we manage the trust?



The organization must function

Operational control → Trust (access)

Access management → automation

PAM technology controls access

Management Analytics

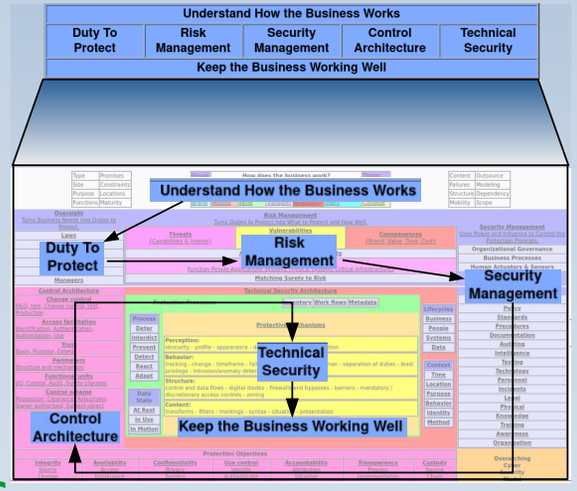
ALL.NET

How do we implement the mix with PAM

There are several levels of trust at issue:

- Trust the decision-makers (implied by their authorities)
- Trust the translation into PAM (how do we translate?)
- Trust PAM technology (the mechanisms of PAM)
- Trust deployed instances

Understand How the Business Works				
Duty To Protect	**Risk Management**	**Security Management**	**Control Architecture**	**Technical Security**
Keep the Business Working Well				



- Duty to protect by management
- Risk management dictates trust levels
- Security management manages the people
- Control architecture sets the “rules”
- Technical security implements the mechanisms

Management Analytics

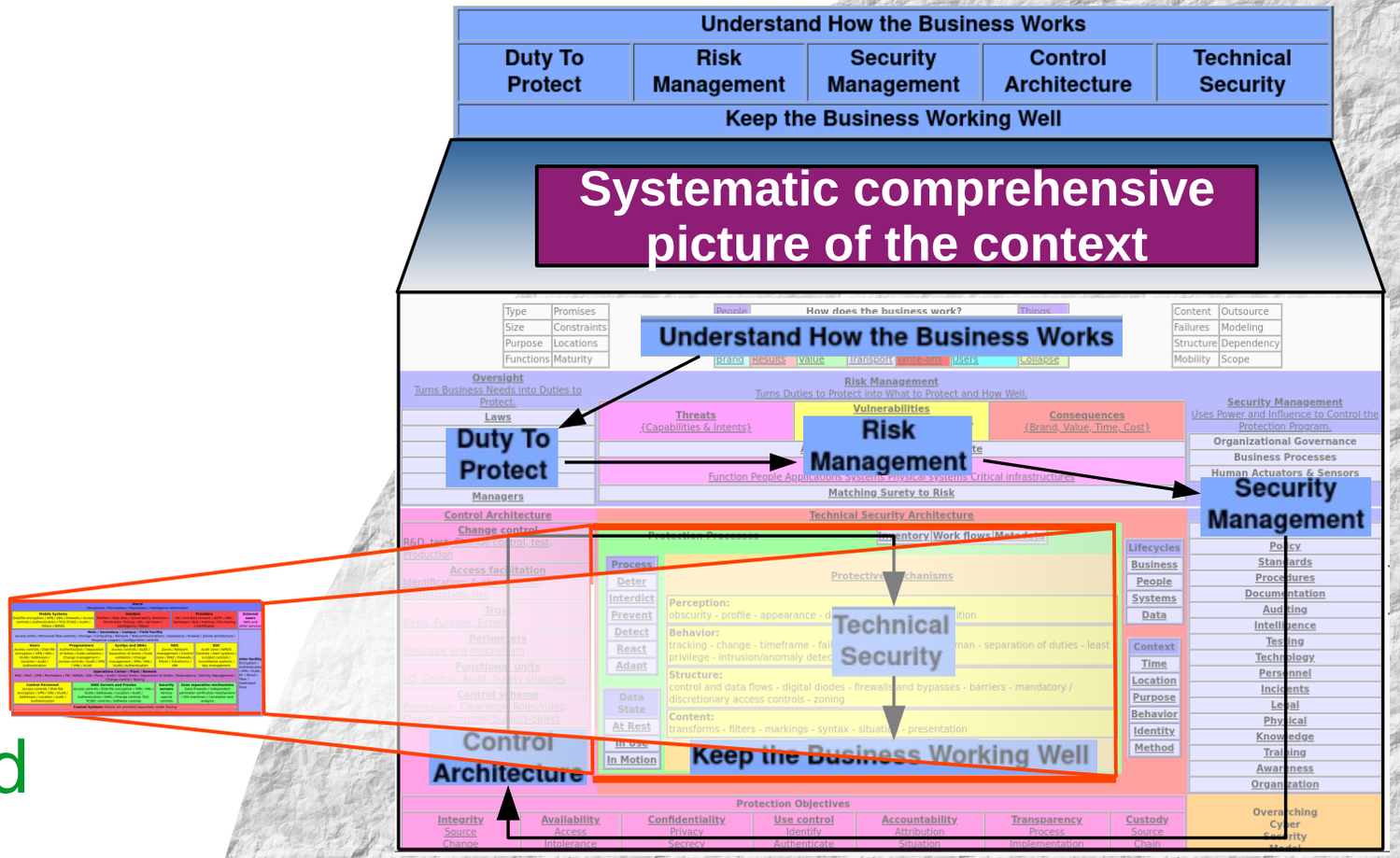
ALL.NET

How do we implement the mix with PAM

Granularity and access control methodology

- Clearances, classifications, and compartments
- Roles and rules
- Attribute-based
- Owner authorized
- Subject/object
- Possession-based
- Mixed models

- **Inventory required**
  - **Trust it?**
- **Workflows required**
  - **Trust it?**



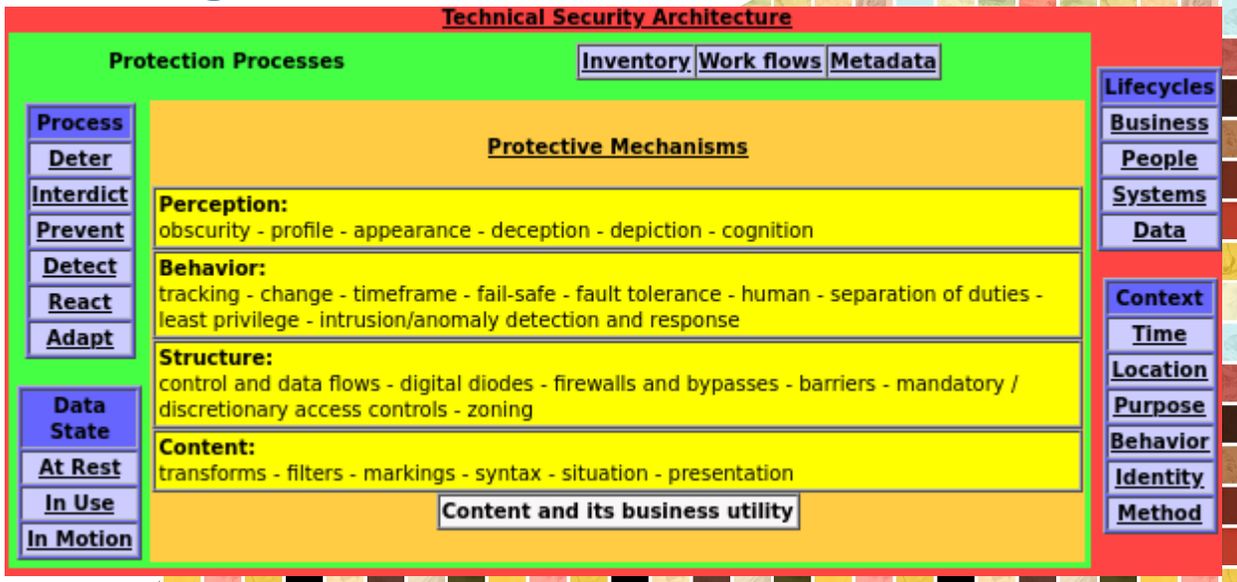
Management Analytics

ALL.NET

How do we mitigate the trust issues?

We don’t mitigate trust issues

- We address them with methodologies
  - Trust models
  - Trust basis
  - Adjudication
  - Risk disaggregation
  - Redundancy
  - Separation of duties
  - Distance and time
  - Matching surety to risk
  - Change control
  - … and more…
- And technical controls…



A much narrower view?

Suppose we just address privilege escalation?

- The question then is under what circumstances do we
  - Escalate privileges to what?
  - De-escalate privileges to what?
- How does this change anything?
  - We need to know and control
    - All of the same things
    - The metrics are even more complicated
      - Because the granularity is high
      - And the implementation is distributed
- And technical controls…
  - Which means identity management
    - Which means IdM systems and mechanisms
      - Which means more trust issues
        - And aggregation and control and …

There will always be mechanisms
They will be imperfect because…
They cannot be perfect!
chmod 755 usr/bin/pkexec

IF you want high leverage
THEN it can be used for good or ill
Learn to live with it

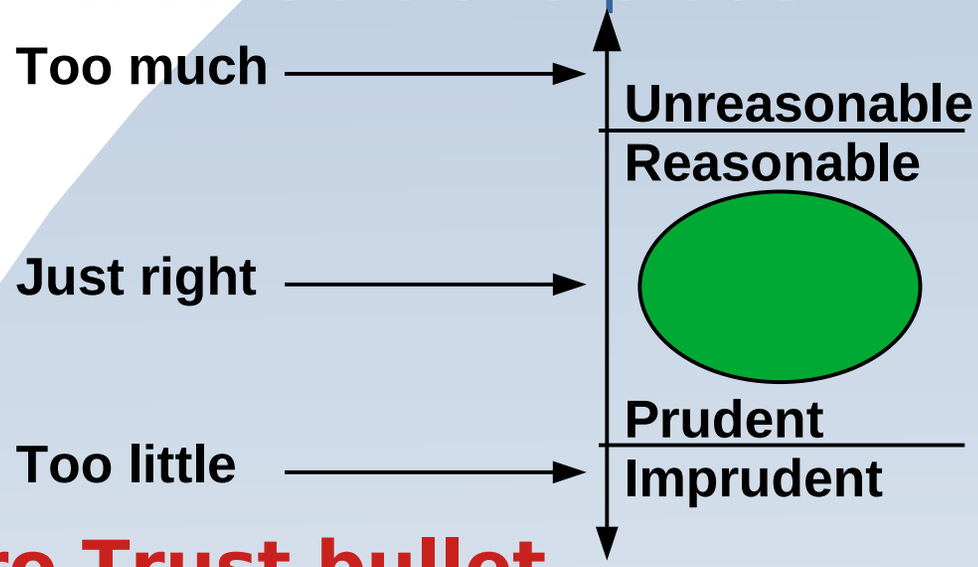
PAM → Non-zero trust

The reality is you need to architect understanding trust

- But let's just admit it…
  - This is a lesson that will not be easily learned

I will still have to do this:
chmod 755 usr/bin/pkexec

- Due diligence requires many reasonable and prudent decisions that are:
  - Situation-dependent
  - Seriously considered
  - By an expert
  - In light of history



- **Don't trust the magic Zero Trust bullet**
  - Be reasonable and prudent and get serious about PAM

Fred Cohen – CEO
Management Analytics
fc@manalyt.com - 831-200-4006